Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 15 June 2005

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports an American Airlines jet flying from New York to Seattle was diverted to Chicago on Monday after a suspicious item was found on board which turned out to be a radio. (See item 7)
- The Washington Post reports that a vital safety system that keeps trains from colliding failed for Metro trains in a Washington, DC tunnel, forcing two quick−thinking train operators to manually stop their trains to avoid a crash. (See item 9)
- Microsoft issued ten security updates for June: three are critical, four are important, and three are moderate. (See item 23)
- The Washington Post reports the Department of Justice's inspector general says the government's new central database for terrorism suspects is missing names, and those omissions heighten the risk a terrorist could go undetected in the United States. (See item 29)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 14, Associated Press* — **U.S. not worried about China's global energy investment, U.S. official says.** China's increasing investment in oil and natural gas projects in Canada and Latin

America to secure supplies for its growing needs isn't a concern to the United States, a senior U.S. energy official said Tuesday, June 14. Guy Caruso, administrator of the U.S. Department of Energy statistical arm, dismissed competition from China in seeking new energy sources, saying Chinese companies have so far only acquired small shares in Canadian oil sands projects. "Huge investments are required, particularly in the Canadian oil sands project ... and it's a free and competitive environment," he said. The need to fuel its expanding economy has taken emerging giant China to Central Asia, Latin America, Africa, the Middle East and even Canada, all areas that the U.S. is counting on to meet its own record−high demand. Some experts warn that the race among governments and companies to secure additional oil and gas assets was expected to intensify amid dwindling global reserves.
Source: http://biz.yahoo.com/ap/050614/malaysia_us_china_energy.html ?.v=1

2. *June 14, Associated Press* — **Energy consumption likely reduced according to energy company.** Energy consumption is likely to be lower this year as global economic growth slows, oil company BP PLC said Tuesday, June 14, giving the industry a breather from the rapid spike in demand that pushed prices higher in 2004. BP Chief Economist Peter Davies said the events that created exceptional energy growth last year −− rapid consumption increases in China and smaller, but still strong, rises in demand almost everywhere else −− were unlikely to continue into 2005. "The key is whether economic growth can remain at 2004 levels," Davies said at a briefing in London on the company's annual review of world energy markets. "It's already evident that the positive combination of forces in 2004 is not continuing with the same momentum through 2005. "Economic growth at a global level has already slowed and is highly probable that 2005 energy consumption will be lower than that in 2004," Davies added. BP said world energy consumption grew by 4.3 percent in 2004, the largest−ever annual increase in global energy consumption in volume terms and the highest percentage growth since 1984.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/14/AR2005061400562.html

3. *June 10, Government Accountability Office* — **GAO−05−379: National Energy Policy: Inventory of Major Federal Energy Programs and Status of Policy Recommendations (Report).** The lives of most Americans are affected by energy. Increased energy demand and higher energy prices have led to concerns about dependable, affordable, and environmentally sound energy. The federal government has adopted energy policies and implemented programs over the years that have focused on the appropriate role of the federal government in energy, attempting to achieve balance between supply and conservation. The May 2001 National Energy Policy (NEP) report contained over 100 recommendations that it stated, taken together, provide a national energy plan that addresses the energy challenges facing the nation. As Congress considers existing federal energy programs and proposed energy legislation in support of the May 2001 report, the Government Accountability Office (GAO) was asked to (1) identify major federal energy−related efforts, (2) review the status of efforts to implement the recommendations in the May 2001 NEP report, and (3) determine the extent to which resources associated with federal energy−related efforts have changed since the release of the NEP report. This report does not contain any recommendations.
Highlights: http://www.gao.gov/highlights/d05379high.pdf
Source: http://www.gao.gov/new.items/d05379.pdf

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *June 14, The Japan Times* — **Fake Yahoo! site nets first phishing arrest in Japan.** A computer−system engineer was arrested Monday, June 13, on suspicion of creating a bogus version of Yahoo Japan Corp.'s Website to steal personal information from users of the nation's largest portal site, police said. It is the first arrest for phishing in Japan, the Tokyo Metropolitan Police Department said. Kazuma Yabuno, a 42−year−old Osaka resident, is facing charges of copyright violation and unauthorized access, after he allegedly created and ran a Website that looked like Yahoo Japan's site −− except the main logo, according to the police. Yabuno, an employee of a computer−system management firm, is also suspected of gaining illegal access to the Yahoo Japan server in late February by using a Yahoo member's account and password obtained from his fake Website, the police said. Yahoo Japan is a Tokyo−based firm that operates an online information portal offering a search engine, auctions, online shopping and other features. According to the police, the Website allegedly created by Yabuno had almost the same design as the genuine one, with the only difference being that the letter "h" in "Yahoo" was replaced with an "f." Member accounts and passwords were automatically forwarded by e−mail to Yabuno's mobile phone.
   Source: http://www.japantimes.co.jp/cgi−bin/getarticle.pl5?nn2005061 4a3.htm

5. *June 13, Internetnews.com* — **Liberty aims to contain identity theft.** The Liberty Alliance Project is stepping up its assault on identity theft with the creation of a new group geared to stymie criminal activity on the Web. The Liberty Identity Theft Prevention Group, which includes Liberty members RSA Security, Nokia, AOL and American Express, say they will fight identity theft around the world. While perpetrators are circumventing technology to keep them out of consumers' private information, consumers aren't helping because of their lack of knowledge about how attacks occur. This is why the group plans to introduce best technological and policy practices and educate consumers and businesses, providing them with the tools they need to make better decisions, said George Goodman, president of the Liberty Alliance management board and a director at Intel. Goodman said that unlike the Federal Trade Commission, which regularly cracks down on cases of identity theft, Liberty is uniquely positioned because it has 44 government, consumer and business groups lending their expertise to one cause: Locking out Web grifters. "At Liberty, we're in a position of looking at public policy issues and business and policy guidelines that go along with the technological aspects of what we do," Goodman said.
   Liberty Alliance Project: http://www.projectliberty.org/

Source: http://www.internetnews.com/dev−news/article.php/3512406

6. *June 13, Computerworld* — **Visa USA adds tool to its credit card antifraud arsenal.** Aiming to reduce credit card fraud, Visa USA Inc. has launched a security tool that allows merchants to instantly check transactions in stores or online, so they can identify fraud before a transaction is completed. In an announcement on Monday, June 13, the San Francisco−based credit card company said its new advanced authorization system is expected to help prevent an estimated $164 million in fraud−related losses over the next five years. Jean Bruesewitz, a senior vice president of processing and emerging products for the company, said advanced authorization adds 10 bytes of additional information to the data sent to card−issuing banks and card−processing companies after a credit card is used. That new information provides a vertical view of the previous and existing spending patterns on the card account and a horizontal look at transactions occurring in real−time across the credit card network. "It looks for unusual patterns of activity [or] anomalies" involving merchants or credit card numbers, Bruesewitz said. Advanced authorization uses algorithms and other mathematical analyses to look for and identify patterns of fraud on the network.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,102472,00.html

[Return to top]

Transportation and Border Security Sector

7. *June 14, Associated Press* — **American Airlines flight diverted to Illinois.** An American Airlines jet flying from New York to Seattle was diverted to Chicago on Monday evening, June 13, after a suspicious item was found on board, authorities said. It turned out to be a radio. A passenger saw the item in one of the plane's restrooms and told a flight attendant, said Chicago Police spokesperson David Banks. The police bomb and arson unit and the FBI determined it was "an older−looking, Walkman−type radio," Banks said. The 158 passengers and six crewmembers were evacuated after the plane landed, said airlines spokesperson Mary Frances Fagan. Flight 289 originated from New York's John F. Kennedy International Airport. The flight crew asked to land at Chicago's O'Hare International Airport so officials there could inspect something on the aircraft, said Chicago Aviation Department spokesperson Kristen Cabanban.
Source: http://www.usatoday.com/travel/news/2005−06−14−flight−divert ed_x.htm

8. *June 14, Reuters* — **High−tech airport missile shield device.** Raytheon Co. unveiled plans Monday, June 13, for a high−tech system to protect airports from attack by shoulder−launched missiles but said the untested device would not be ready for deployment for at least 18 months. The system, which is named Vigilant Eagle, is a response to fears of attacks on airliners after shoulder−fired missiles were launched at an Israeli plane three years ago. Such a system would likely be necessary to reopen Baghdad's airport to civil air traffic. The form of attack has been a concern for airlines and a hot topic for defense contractors since two missiles were unsuccessfully fired at an Israeli airliner in Mombasa, Kenya, in November 2002. A year later, a DHL cargo jet was hit by a shoulder−fired missile in Baghdad. The system works by a network of infra red sensors set up around an airport detecting a fired missile, and then relaying information to a microwave device, about the size of a billboard, which directs electromagnetic waves at the missile to disrupt its operation and deflect it away from the aircraft.

Source: http://money.cnn.com/2005/06/14/news/fortune500/raytheon.reu t/

9. *June 13, Washington Post* — **Trouble in tunnel delays Washington's Metro.** A vital safety system that keeps trains from colliding failed last week in the tunnel between Washington, DC's Foggy Bottom and Rosslyn, VA, forcing two quick−thinking train operators to manually stop their trains to avoid a crash, Metro officials said on Sunday, June 12. Until engineers figure out what caused the failure, transit managers have ordered all trains using the tunnel to operate manually, which is causing delays and crowding along the Blue and Orange lines. "Until we can find the problem in the circuit and correct it, until we can replicate what happened so we can find the cause of it and fix it, we're running in manual," said Jim Hughes, Metro's acting deputy general manager for operations. Metro's trains are run by onboard computers, which communicate with relays along the track bed and control train speed and braking. Another electronic system, called train separation, detects the position of trains and makes certain that a safe distance is maintained between them. That system forces a train to stop if it gets too close to another. The failure of the track circuit is highly unusual. Metro officials could not remember another instance when the train separation system did not perform, Hughes said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/13/AR2005061301564.html

[Return to top]

Postal and Shipping Sector

10. *June 14, St. Petersburg Times (FL)* — **Cargo plane crash−lands on street.** The vintage DC−3 cargo plane was in trouble moments after it took off from the Fort Lauderdale Executive Airport when one of the two engines caught fire. Seconds later, the plane smashed down on a street and skidded about 100 yards, narrowly missing several houses. The wings smashed trees and dug through lawns and driveways. Amazingly, the two pilots and the lone passenger scrambled free before the plane turned into a fireball. All three people from the plane and two from the ground were taken to area hospitals. In a neighborhood that includes a medical center, high school, and other buildings, officials said the incident could have erupted into a full−blown disaster. The plane, bound for Marsh Harbor in the Bahamas with 3,200 pounds of granite aboard, went down about three miles east of the airport, minutes after it took off. The cause of the crash is under investigation. Co−pilot Charles Wirt told firefighters he thought a fuel line broke, which caused the engine to catch fire.
Source: http://www.sptimes.com/2005/06/14/State/Plane_crash_lands_on_.shtml

[Return to top]

Agriculture Sector

Nothing to report.
[Return to top]

Food Sector

11. *June 10, Food and Drug Administration* — **Tuna recalled in New York due to listeria contamination.** Golden Taste, Inc. is recalling its Golden Taste Tuna Deluxe in 7.5 ounce and 3.5 ounce clear plastic containers because they may be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people and others with weakened immune systems. The recalled Golden Taste Tuna Deluxe was distributed to retail stores throughout New York State. The product is coded 7/03/05. No illnesses have been reported to date in connection with this problem.
Source: http://www.fda.gov/oc/po/firmrecalls/goldentaste06_05.html

12. *June 07, Virginia Tech* — **University awarded grant to study high pressure treatment to inactivate Norwalk virus.** The U.S. Department of Agriculture's Cooperative State Research, Education, and Extension Service (USDA/CSREES) announced that Virginia Tech, in collaboration with the USDA/ARS Microbial Safety of Aquaculture Products Center of Excellence, Dover, DE, and the Rollins School of Public Health at Emory University, Atlanta, GA, were awarded a grant to study the effects of high hydrostatic pressure in inactivating Norwalk virus, using oysters as a model. Norwalk and Norwalk−like viruses (collectively 'noroviruses') are the most common cause of foodborne disease outbreaks in the United States with 22 million cases reported annually. The disease is characterized by nausea and gastroenteritis, and usually passes in two to three days with no long term effects. The disease is rarely fatal, but dehydration can become dangerous in rare cases. In the United States, most outbreaks are linked to consumption of raw oysters and clams, contaminated water, raw salads, and ready−to−eat foods. Noroviruses are resistant to detergents, solvents, high temperatures and freezing, and are extremely contagious. The research team will identify one or more high pressure processing schedules resulting in virus inactivation.
Source: http://www.vtnews.vt.edu/Story.php?itemno=827

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

13. *June 14, innovations report* — **A molecule impedes the destruction of the Brucella bacteria.** Research carried out with the participation of the University of Navarra in Spain has shown how a determinate molecule helps an important pathogen, Brucella abortus, escape destruction within the cells charged with eliminating infectious agents (macrophages). This research has been published in Nature Immunology scientific magazine. Brucella is a model of an intracellular parasite, a category that includes other important bacteria, such as those of tuberculosis or legionelosis. Brucellosis, the illness caused by these bacteria, is of great importance worldwide, with millions of human beings and domestic animals affected.
Nature Immunology (subscription only): http://www.nature.com/ni/journal/v6/n6/index.html
Source: http://www.innovations−report.com/html/reports/life_sciences /report−45352.html

14. *June 14, News−Medical.Net* — **New gene identification technology developed at Cornell University.** New technology developed at Cornell University, IL, could make it easy to identify genes, pathogens, illegal drugs and other chemicals of interest by tagging them with color−coded probes made out of synthetic tree−shaped DNA. A research group headed by Dan Luo, Cornell assistant professor of biological engineering, has created "nanobarcodes" that fluoresce under ultraviolet light in a combination of colors that can be read by a computer scanner or observed with a fluorescent light microscope. Other methods of identifying biological molecules that are available or being developed mostly involve expensive equipment, Luo said. "We wanted something that could be done with inexpensive, readily available equipment," he said. The researchers have tested their system using samples containing various combinations of E. coli, anthrax and tularemia bacteria and ebola and SARS viruses, and have found the color codes could clearly distinguish several different pathogens simultaneously. The research is described in a paper, "DNA fluorescence nanobarcodes for multiplexed pathogen detections" to be published in the July 2005 issue of the journal Nature Biotechnology.
Nature Biotechnology (subscription only): http://www.nature.com/nbt/index.html
Source: http://www.news−medical.net/?id=10973

15. *June 14, National Institutes of Health* — **Promising new TB drug enters clinical trial.** A promising new drug candidate that may be effective against both actively dividing and slow−growing Mycobacterium tuberculosis (M. tb) has begun testing in humans, the National Institute of Allergy and Infectious Diseases (NIAID), part of the National Institutes of Health, announced Tuesday, June 14. The novel antibiotic, PA−824, may shorten the time needed to treat tuberculosis (TB), a contagious disease that claims approximately two million lives worldwide each year. In partnership with the non−profit New York−based Global Alliance for TB Drug Development (TB Alliance), NIAID contributed to the drug candidate's preclinical safety and efficacy testing in animal models. Now, a clinical trial to assess PA−824's safety, sponsored by the TB Alliance, has opened at a medical clinic in Lincoln, NE. One−third of the global population — some two billion people — is infected with M. tb. Although most common in other countries where HIV prevalence is highest, approximately 14,000 cases of active TB are reported to the Centers for Disease Control and Prevention each year in the United States. While TB is curable with antibiotics, the drug regimen is arduous and lengthy.
NIAID TB information Website: http://www.niaid.nih.gov/Newsroom/FocusOn/TB/default.htm
Source: http://www.nih.gov/news/pr/jun2005/niaid−14.htm

16. *June 13, internetnews* — **Fake Canadian drug sites proliferating.** Almost 80 percent of sites purporting to offer Canadian pharmacy prescription drug sales are registered in other countries, according to data released today by Cyveillance. The online risk management firm conducted the study for the Food and Drug Administration (FDA). Using a master list of 60 million domain names, Cyveillance discovered approximately 11,000 sites that were designed to appear as Canadian pharmacy sites. Of those sites, a little more than a thousand actually sold prescription drugs. Of those sites, only 214 had registration data containing a Canadian address or exhibited any data suggesting they were hosted by a Canadian Internet service provider. Todd Bransford, spokesperson for Cyveillance, said a lot of the companies were based in the United States. "One company had 384 sites implying they were Canadian drug firms," he said. Other countries found to be hosting pseudo Canadian sites included Barbados, Mexico, the

Czech Republic, El Salvador, Australia and Vietnam. While legitimate U.S. Internet pharmacies provide safe access to prescription drugs, foreign Internet pharmacies operate outside of U.S. law and are not subject to FDA standards.
Cyveillance Press Release: http://www.cyveillance.com/web/newsroom/press_rel/2005/2005−06−13.htm
Source: http://www.internetnews.com/xSP/article.php/3512436

[Return to top]

Government Sector

17. *June 13, Government Computer News* — **Forrester study finds slowing e−government adoption.** The Presidential e−Government Initiatives of 2000 have lost much of their steam because people still prefer to interact with federal agencies over the telephone, according to a report from Forrester Research Inc., of Cambridge, MA. “Our research indicates that citizens contact the government predominantly for personal rather than business reasons, seeking answers to specific questions, expressing opinions or completing transactions,” said Alan Webber, a consulting analyst. “Because of the personal nature of these interactions, they still rely on telephone and in−person contact and don’t completely trust the Web. Hurdles for implementation of e−government initiatives include constrained budgets and a change−resistant culture, which may become exacerbated as federal IT spending begins to decrease in the next couple of years, the report said. Government bureaucracy, extremely long project cycles and long overdue deadlines also have slowed adoption. Moving forward will require more disciplined management practices, an increase in the security of online environments, more complete enterprise architectures, greater capabilities for records and data, and additional IT talent, according to the study.
Forrester Research Website: http://www.forrester.com/
Report information: http://www.forrester.com/Research/Document/Excerpt/0,7211,36950,00.html
Source: http://www.gcn.com/vol1_no1/daily−updates/36068−1.html

[Return to top]

Emergency Services Sector

18. *June 13, Government Technology* — **New Jersey to expand statewide intelligence management system.** The New Jersey Department of Law and Public Safety has purchased a statewide site license to support the expansion of its Statewide Intelligence Management System (SIMS). The system will enable the Office of Counter−Terrorism and New Jersey State Police to connect the dots between local crimes that can serve as precursors of terrorist activity, such as money laundering and obtaining fraudulent identification. The system will also enable State Police to connect local gang activities such as the street sale of drugs to larger, organized criminal ventures. SIMS represents the first operational intelligence system to be deployed throughout a U.S. state. Highly flexible, SIMS employs a comprehensive database to collect and share information on suspected involvement in all types of organized criminal activity. The system allows agencies to store their intelligence for their own use or for use by the entire law

enforcement community, serving the varying needs of multiple users and methods of sharing intelligence. Training and access to the system is managed by the State Police and offered free to all qualified agencies.
Source: http://www.govtech.net/magazine/channel_story.php/94281

19. *June 13, The Gazette (MD)* — **Emergency training exercise to be held at Maryland high school.** A training exercise will be conducted by Emergency Management officials in Laurel, MD, to test city's response to an "active shooter" inside Laurel High School on Saturday, June 18. The training will involve reports of subjects inside the school with guns, and reports of students being shot. The Laurel Police Department's Emergency Response Team will be dispatched to the school, and the training there will test the strengths and weaknesses of all departments−−police, fire and rescue, public works, Community Emergency Response Team and public information. City, county and state officials will be evaluating the drill.
Source: http://www.gazette.net/200523/princegeorgescty/updates/27985_8−1.html

20. *June 13, Daily American Republic (MO)* — **Bioterrorism training challenges local, state emergency responders in Missouri.** Missouri Department of Natural Resources emergency responders from across the state converged on Wappapello State Park last week for hands−on training that culminated with the discovery of a simulated bioterrorism lab. Assisting DNR's environmental emergency responders (EER) were members of the Missouri Army National Guard's 7th Civil Support Team from Fort Leonard Wood, the FBI, the local Ozark Regional Hazardous−Materials/Weapons of Mass Destruction team, the Sikeston Department of Public Safety and the U.S. Army Corps of Engineers. The objectives for the training were to see how DNR personnel integrated into unified command and to give "suit time for our personnel," explained Alan Reinkemeyer, DNR EER section chief. One area that "failed," according to DNR state on−scene coordinator Randy Carter, was staging. Responders were supposed to report there before being sent into operations and given assignments on the entry teams.
Source: http://www.darnews.com/articles/2005/06/13/news/news10.txt

21. *June 13, Los Alamos Monitor (NM)* — **Lecture outlines airborne hazard detection system.** A one of a kind airborne hazard detecting system onboard a sleek aircraft was the highlight of a dynamic lecture presented by the Center for Homeland Security (CHS) Wednesday, June 8, at Los Alamos National Laboratory. The system is called ASPECT for "Airborne Spectral Photometric Environmental Collection Technology." It detects chemicals, radiological materials, collects high−resolution digital and video photography and takes thermal and night images. Undergraduate scholars and graduate fellows from a Department of Homeland Security program are participating in the 10−week seminar series this summer. Los Alamos scientists provide the technology of ASPECT's unique computer pattern recognition tools. The Environmental Protection Agency's disaster first−responder crew operates the aircraft. The system's information combines with high−resolution digital imagery and Global Positioning System (GPS) information to create a map of land surface and plume hazard. ASPECT shows gas collections in low−lying areas and locations with little air movement. The system parachutes a terminal and cell phone to responders and downloads data to a wide range of wireless networks. ASPECT has been deployed 44 times over the last couple of years on missions ranging from a chlorine−spilling train derailment near San Antonio to the 2002 Winter Olympics in Salt Lake City.
Los Alamos Center for Homeland Security: http://www.lanl.gov/orgs/chs/index.shtml

Source: http://www.lamonitor.com/articles/2005/06/13/headline_news/n ews04.txt

22. *June 07, University of California, San Diego* — **Computer scientists develop wireless application for 3D video.** Computer scientists at the University of California, San Diego (UCSD), have developed a new technique for mixing images and video feeds from mobile cameras in the field to provide remote viewers with a virtual window into a physical environment. Dubbed 'RealityFlythrough,' the application constructs a 3D virtual environment dynamically out of the live video streams. "Instead of watching all the feeds simultaneously on a bank of monitors, the viewer can navigate an integrated, interactive environment as if it were a video game," said UCSD computer science professor Bill Griswold, who is working on the project with Ph.D. candidate Neil McCurdy. The researchers at UCSD's Jacobs School of Engineering have already begun testing the software for homeland security and emergency response. During a May 12 disaster drill organized by San Diego's Metropolitan Medical Strike Team, the researchers shadowed a Hazmat team responding to a simulated terrorist attack. They wore cameras mounted on their hardhats, tilt sensors with magnetic compasses, and global positioning (GPS) devices. Walking through the simulated disaster scene at the city's Cruise Ship Terminal, they captured continuous video to be fed over an ad hoc wireless network to a makeshift command post nearby.
Source: http://ucsdnews.ucsd.edu/newsrel/science/RealityFlythrough.a sp

[Return to top]

Information Technology and Telecommunications Sector

23. *June 14, Microsoft* — **Microsoft issues June security bulletin.** Microsoft issued its security update for June on Tuesday, June 14. Of the ten updates (MS05−025 – MS05−034) issued for June, three are critical, four are important, and three are moderate. Affected products and components are Internet Explorer, Windows HTML Help, Windows Server Message Block, Web Client Server, Outlook Web Access for Exchange Server, Outlook Express, Step−by−Step Interactive Training, Microsoft Agent, Telnet Client, and ISA Server 2000. Impacts include remote code execution, information disclosure, and escalation of privilege. See Source link and individual bulletins for updates.
Source: http://www.microsoft.com/technet/security/bulletin/ms05−jun. mspx

24. *June 13, Secunia* — **e107 eTrace plugin shell command injection vulnerability.** A vulnerability in the eTrace plugin for e107, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "etrace_cmd" and "etrace_host" parameters in "dotrace.php" isn't properly sanitized before being used in a "system()" call. This can be exploited to inject arbitrary shell commands. There is no solution at this time.
Source: http://secunia.com/advisories/15678/

25. *June 13, SecurityFocus* — **OpenSSL ASN.1 parsing vulnerabilities.** Multiple vulnerabilities were reported in the ASN.1 parsing code in OpenSSL. These issues could be exploited to cause a denial of service or to execute arbitrary code. To successfully exploit this vulnerability, an attacker must force a computer to decode malformed ASN.1 data. Refer to Source link below for vendor solutions.

Source: http://www.securityfocus.com/bid/8732/solution

26. *June 13, SecurityTracker* — **Symantec pcAnywhere 'Launch With Windows' properties let local users gain elevated privileges.** A vulnerability was reported in Symantec pcAnywhere. A physically local user can modify the Caller Properties of the Host Properties Settings for the 'Launch with Windows' feature to cause arbitrary commands to be executed when the system is restarted. The commands will run with Local System privileges. The vendor has released a patch. For consumer versions of Symantec pcAnywhere: http://www.symantec.com/techsupp/files/pca/index.html For enterprise versions of Symantec pcAnywhere: http://www.symantec.com/techsupp/enterprise/products/spca/fi les.html
Source: http://www.securitytracker.com/alerts/2005/Jun/1014178.html

27. *June 12, SecuriTeam* — **WebSphere Application Server Administrative Console buffer overflow.** A buffer overflow in the WebSphere Application Server Administrative Console allows attackers to execute arbitrary code from remote. The security vulnerability exists in the authentication mechanism. The authentication process takes place only when the 'global security option' is enabled in the server. The vulnerability cannot be exploited if the security option is disabled. Apply the WebSphere Application Server 5.0.2 Cumulative Fix 11: http://www−1.ibm.com/support/docview.wss?rs=180&uid=swg24009 775
Source: http://www.securiteam.com/securitynews/5WP0C0KG0S.html

28. *June 11, SecurityFocus* — **Pico Server buffer overflow and directory traversal vulnerabilities.** Two vulnerabilities were identified in Pico Server (pServ), which may be exploited by remote attackers to execute arbitrary commands or gain unauthorized access. The first issue is due to a heap overflow error when processing long CGI arguments. The second vulnerability is due to an input validation error when handling specially crafted HTTP requests containing "/./../" sequences. Upgrade to version 3.4: http://pserv.sourceforge.net
Source: http://www.securityfocus.com/bid/13935/discuss

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports Microsoft Security Bulletins for June, 2005 address a number of vulnerabilities in Windows, Internet Explorer, Outlook Express, Outlook Web Access, ISA Server, the Step by Step Interactive Training engine, and telnet. Exploitation of the most serious of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. This would allow an attacker to take complete control of a vulnerable system. An attacker could also execute arbitrary code with user privileges, or cause a denial of service. Further information about the more serious vulnerabilities is available at URL:

http://www.us-cert.gov/cas/techalerts/TA05-165A.html

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 6881 (bittorrent), 27015 (halflife), 53 (domain), 1026 (---), 139 (netbios-ssn), 25 (smtp), 6882 (---), 1025 (---) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

29. *June 14, Washington Post* — **Inspector General review of terrorism database released.** The government's new central database for terrorism suspects is missing names, and those omissions heighten the risk a terrorist could go undetected in the United States, the Department of Justice's inspector general says. In addition, in one instance last year, someone on the government's no-fly list was allowed to board a domestic airline flight because of poor coordination between the FBI-run Terrorist Screening Center and other law enforcement agencies, Inspector General Glenn A. Fine said on Monday, June 13. Fine also found some names that were mistakenly included in the database. Still, he praised the ambitious effort to merge about a dozen terrorist watch lists from nine agencies. Donna A. Bucella, the center's director, said problems identified by Fine have been corrected and noted that she had requested the audit. The center was designed as a one-stop shop that any government official can consult to check the name of someone who has been screened or stopped. The merged databases include the Transportation Security Administration's no-fly list of terrorist suspects barred from air travel; the State Department's massive Tipoff list, which is checked when visas are issued; and the FBI's National Crime Information Center list of convicted felons, fugitives and other wanted people, and used by police nationwide.
Report: http://www.usdoj.gov/oig/special/0506/final.pdf
FBI Statement: http://www.fbi.gov/pressrel/pressrel05/06132005.htm
Source: http://www.washingtonpost.com/wp-dyn/content/article/2005/06/13/AR2005061301454.html

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.